Division of Health Care Finance and Policy Security Measures

The Division of Health Care Finance and Policy (the Division) applies many layers of security and is constantly reviewing them for improvement. The Division employs comprehensive security to all aspects, from physical building security, to network security and ultimately to the data itself. Data obtained for specific uses from external entities is only used for the specific purpose for which it was obtained. Any data submitted by external entities that contains confidential data under the Fair Information Practices Act is protected from disclosure. All requests for access to confidential data are reviewed by the Division's Data Protection Committee.

The Division has several layers of physical security, building access, server room access and controls and procedures to support the infrastructure. The building has security guards in the main lobby, controlling access to the elevators. These guards also have cameras that monitor all the entry doors to the building. The server room is located on the 5th floor. The 5th floor has a receptionist at the entrance to the floor that checks all visitors before they can enter the floor. There are also security cameras that monitor the reception area and more cameras that monitor the area directly outside the server room, with still another camera inside the server room. All the activity captured on these cameras is stored and available for further review, if necessary. The server room is secured by an audited lock system that is controlled by employee ID badges. In the entire Division, there are only 4 badges that have access to the server room, and the system logs and tracks every entry and exit. There are also cameras on the 4th floor that record the main entrance and hallway. All cameras are configured so they will continue to operate even if one or more fails.

If someone comes in and tries to plug in a computer that is not known to the Division's network (laptops or any computer that is brought in), it is not permitted to access the Division's network. If someone attempts to connect a laptop or device to the network they will be unable to get anywhere. The system will assign them a sandbox IP and restrict all access. Network software immediately recognizes any device that connects to it and checks the security tables to identify the device and determine if it has been granted access from the Division's network support group. The network support group will be automatically notified of this action, via a message to their blackberries. All important events are configured to automatically message the support team's blackberries, so that no alert goes unnoticed or waits until someone finds it. Besides the physical computer access, each person or application must identify and authenticate itself with a user ID and password. These credentials are necessary to access the basic network. Once on the network, all access is controlled by these credentials. Access to folders, files, applications, reports and data is controlled to an individual level and further controlled by policies and procedures. Even internal staff requires signed authority to access confidential information and is time sensitive according to the time to perform the assignment. As part of every employee's orientation, they go through a confidentiality awareness session and sign the confidentiality form, confirming their awareness and agreement to the terms and conditions. This activity is repeated on an annual basis. People that fail to authenticate in 3 tries are locked out of the network until a network support member resets their account. A long with this feature, the Division has software that enforces strong passwords and requires the password to be changed every 45 days.

The Division employs several software products to assist in immediate identification of alerts and to assist staff sifting through and analyzing all the audit trails and log files that track network and application activity. These products not only make it possible to review such large amounts of information in a timely manner, but also enforce the policies and rules of the Division. These tools monitor software and hardware to ensure they are operating properly and that they stay current with all updates and patches. As industry leading products, they offer suggestions to assist in spotting suspicious activity and offer best practices. See attachments for further information about 3 of the products currently in use to protect the network and data.

The Division operates a Microsoft windows network using Active Directory (AD). This too enables the Division to create detailed user definitions and utilize this for policy enforcement and granular security. The database is SQL server and the Division utilizes all built-in security features to restrict and monitor access, as well as encryption. To go a step further, The Division operates a third party product that further enhances the security features of both AD and SQL server. If any changes are made to the security, permissions, registry settings and other key information, this software will alert staff and will take immediate action based on the alert type. The software will mitigate problems using built-in security best practices. This means there is real time monitoring, collection, analyzing, alerts, and mitigation of network and software issues.

Idera SQLsecure

Security Analysis & Reporting

Effective Rights Analysis – analysis of users' effective rights shows you how and where each right is granted, making it easy to pinpoint exactly what changes need to be made in order to close security holes.

Database Roles Permissions – view sub-roles, role members, assigned and effective permissions.

SQL Server Files, Directories, and Registry Settings – browse and analyze all files, directories and registry settings associated with SQL Server and determine ownership as well as explicit and inherited security rights.

Services – Show details of services such as logon and configuration.

SQL Server Surface Area and Protocols – disables unused components to reduce exploit risks.

OS Security Analysis – assess the OS setup to identify issues that would compromise SQL Server security.

Powerful User Analysis – analyze membership to powerful server roles and groups such as administrators, system administrators and security administrators so you can ensure this level of access is warranted.

Security Scorecard – lists potential security concerns on your SQL Servers such as cross database chaining and gives you the ability to drill down to view the full details.

Detection of Unresolved Windows accounts – SQLsecure shows you all logins on the target server, as well as any unresolved Windows accounts or groups.

Server Security Properties – show all security related properties for servers including: version and patch level, authentication mode, audit mode, proxy account, and cross database chaining.

Comprehensive Security Model Version History and Baselining – the SQLsecure Repository keeps a complete history of SQL Server security settings, providing the ability to designate a baseline to compare against future snapshots to detect changes. This also provides a valuable audit trail for forensic analysis.

Powerful Reporting – use built-in standard reports for security auditing and compliance; plus, produce custom reports or perform custom analysis via the data stored on the SQLsecure repository.

Data can also be exported to Excel.

Cross-server Reporting – provides the ability to show security state from a global view (e.g. all instances with guest accounts enabled).

New in Version 2.0

Policies – checks over 60 key security standards across your entire enterprise. Contains built in policies from NIST, DISA, CIS, and others. Or you can create your own.

Dashboard – allows you to check and see where your enterprise of SQL Servers stands at a glance. Drill down into the details of the issues. See how to remediate problems.

Alerts – upon collection assesses your security state the according to your standards and alerts you if anything fails to meet that standard.

Database Roles Permission Explorer – view sub-roles, role members, assigned and effective permissions.

SQL Server Files, Directories, and Registry Settings – browse and analyze all files, directories and registry settings associated with SQL Server and determine ownership as well as explicit and inherited security rights.

Services – show security details of services such as logon and configuration.

SQL Server Surface Area and Protocols – disables unused components to reduce exploit risks.

OS Security Analysis – assess the OS setup to identify issues that would compromise SQL Server security.

Security Scorecard – lists potential security concerns on your SQL Servers such as cross database chaining and gives you the ability to drill down to view the full details.

Reporting Enhancements – includes new comprehensive risk assessment report, many new reports, and enhancements to all reports. Added charts for visualization. Allows you to group servers in the reports by policy group containment.

CFI Network Server Monitor

Enterprise class architecture

GFI Network Server Monitor consists of a network monitoring service and a separate management interface. No agent software needs to be installed on the machines you wish to monitor. The Network Monitor Engine is multi-threaded and can run 40 checks at a time. This software architecture allows for high reliability and scalability to monitor both large and small networks.

Includes checks for Exchange 2000/2003, ISA server, IIS and others

Via the Quickstart wizard, you can quickly create a series of checks which monitor all the important services on your network, including Exchange Server, IIS and others. Critical Exchange services and performance counters (Information Store, mailboxes, SMTP service, etc) are monitored.

Monitors terminal servers by actually logging in

GFI Network Server Monitor can check the status of a terminal server by actually performing a complete login and checking if the session is established correctly. This monitoring method is superior to relying on the events that the terminal server generates (as Microsoft MOM does).

Monitor your database servers (SQL/ODBC)

GFI Network Server Monitor can check the availability of all leading database applications. Out of the box, it can monitor Microsoft SQL Server via ADO. Other databases such as Access, FoxPro, Paradox, SyBase, Informix, IBM DB2 and many more can be monitored via ODBC.

Monitor Linux servers

GFI Network Server Monitor includes extensive checks for monitoring Linux servers. You can monitor CPU usage, printer availability, file existence, process running, folder size, file size, users and groups membership, disk partition check and disk space. In addition, administrators can create any check by creating an SSH script.

Performs administrative steps to ensure that a service is running

GFI has developed specialized checks which mimic administrator operations to verify that services offered by various applications are running, for example, logon to a service, perform a task and logoff the service – without the need for any administrative intervention! The monitoring functions that make use of such methodologies include: IMAP, POP3, SMTP Server and the email route check. Through the active use of such services one can guarantee that all aspects of these services are running and functioning.

Takes corrective action automatically

After an unexpected condition has occurred, GFI Network Server Monitor can automatically correct the problem by restarting a service (or multiple services) upon failure; rebooting a server upon failure; or launching an executable, batch job or VBScript.

Built-in computer monitor functions

- CPU usage function – Ensure that a processor’s usage does not go beyond a certain level
- Performance counter – Monitor any internal operating system counter, including counters used by SQL Server and MSMQ
- Directory size function – Ensure that a particular directory (for example, a user’s home directory) does not take up more than x amount of drive space
- Disk drive function – Monitor the physical status of the disk
- Disk space function – Check if sufficient disk space is available
- File existence function – Monitor the existence of a particular file, for example, results of scheduled batch jobs
- File size function – Monitor the size of particular files, for example, critical log files.

Built in Internet service functions

- HTTP function – Checks availability of HTTP and HTTPS sites; passes credentials if required
- Website content checking – Checks website content by specifying a text pattern
- FTP function – Checks availability of an FTP server/site
- ICMP ping function – Checks a remote host for availability
- IMAP server function – Checks that the IMAP service is functioning by logging into the service and checking the count of the emails contained in a specific folder on the IMAP server
- DNS server function – Checks DNS server by reading an 'A' record and verifying the result
- SMTP server function – Checks mail server by establishing a connection and handshaking to verify SMTP protocol is working correctly
- POP3 server function – Checks POP3 servers by establishing a connection and handshaking
- NNTP news server function – Checks connection and does a handshake
- SNMP function – Monitors specific variables on remote machines or devices via the SNMP GET message
- TCP port function – Checks if a port is responding and checks its response
- NTP timeserver function – Monitors status of timeservers
- Email route function – Checks the health of email services by actually sending test emails and verifying their delivery at destination. This check is also useful for verifying performance of your mailing systems
- Daemon function – SSH-based check that verifies if particular daemons are running on target Linux/Unix computer/s.

Alert notification via email, pager or SMS

When it detects a failure, GFI Network Server Monitor can send alerts via SMS, pager, email or a network message. SMS (text) messages are sent either through an SMS service provider (SMSC), directly through a connected GSM phone/modem; it is also possible to use the GFI FAXmaker email-to-SMS gateway service, Clickatell’s web email-to-SMS online gateway service or any third party email-to-SMS gateway. All notifications can be customized using variables. Recipients can be configured globally for all rules.

Support for SQL Server/MS Access as a database backend

GFI Network Server Monitor allows you to store monitoring data to either an SQL Server or MS Access database backend. SQL Server is more appropriate for users with higher monitoring level requirements as well as those who need to centralize the monitoring results of multiple GFI Network Server Monitor installations in one place (such as backups, remote accessing as well as report generation by third party tools such as Crystal Reports or MS Reporting Services).

View network status from anywhere in the world

You can check rule status from any location using GFI Network Server Monitor's remote web monitor. The remote web monitor includes two types of web page views: One for a normal web browser and one optimized for viewing from a mobile phone or handheld device such as a BlackBerry or a Palm. A small footprint web server is included, although the feature can also be operated in conjunction with IIS.

Monitor remote event logs

GFI Network Server Monitor can scan Windows event logs on local or remote computers and look for specific event sources, categories, event IDs and patterns in the description of the event. In addition, it can look for multiple events occurring in a specific time interval, for example, a McAfee or Norton virus alert posted in the last 30 minutes.

Monitor processes, services performance and CPU usage

GFI Network Server Monitor enables you to check critical processes and services on local and remote computers. You can also monitor the CPU usage of a machine and any performance counter accessible through perfmon.msc. This way, you can ensure that virtually any application is running properly.

Custom network monitoring using VBScript and SSH

Although GFI Network Server Monitor includes an extensive set of default monitoring functions, you can build your own custom checks by writing a VBScript (Windows) or an SSH shell script (Linux). From VBScript, you can use both WMI and ADSI. WMI is an interface to a broad range of hardware/software/OS-related properties of a computer, allowing you to perform almost any check. Using ADSI, you can interface to Active Directory.

Monitor users, groups and other Active Directory information

Use GFI Network Server Monitor to monitor directory information. For example, monitor group membership of the domain admins group. You can also check user accounts (locked out, disabled, etc.), computer accounts, groups, group membership, organizational units, and so on.

Competitively priced

Network monitoring/management products are traditionally rather expensive. By contrast, GFI Network Server Monitor costs just USD 1,530 to monitor up to 50 IPs and USD 594 to monitor up to 10 IPs.

Nested folder support

It is possible to organize folders in a nested folder format - this provides support for more complex monitoring needs such as that of consultants or enterprises with more granular server distribution.

Other features

- Configure maintenance periods to avoid alerts being sent during scheduled maintenance
- Advanced logging options to text file or event log
- Configure dependencies to avoid multiple alerts for error conditions dependent on each other
- Monitor network printer status
- Reporting – includes reports that detail the availability of your network resources; alternatively, use Crystal Reports to access the database and create your own reports
- Monitoring checks wizard that easily configures new checks for your present systems
- Accommodates employee shifts: GFI Network Server Monitor can notify different people depending on the time at which the check triggered.

GFI Events Manager

The huge volume of system events generated daily is a valuable source of information for organizations to meet legal and compliance obligations and address IT security risks. Growing threats to business continuity calls for an approach that includes real-time monitoring of the network and also the ability to report and analyze this data to meet stringent and more demanding legal or compliance obligations.

Many companies mistakenly assume that unauthorized access is only attempted by external parties. Actually, the majority of corporate security threats stem from internal sources, against which a firewall offers no protection.

A good security strategy includes real-time monitoring for critical security events and periodic analysis of your systems' security logs so that you can detect and respond in a timely fashion to internal and external attacks. In fact, when reviewing the general controls of a corporation, public auditors and regulatory agencies define security-log monitoring as a necessary best practice and a part of performing due diligence.

GFI EventsManager is an events monitoring, management and archiving solution that helps organization meet legal and regulatory compliance such as SOX, PCI DSS, and HIPAA. This award-winning software supports a wide range of event types such as W3C, Windows events, Syslog and, in the latest version, SNMP traps generated by devices such as firewalls, routers and sensors as well as custom devices

> Centralizes Syslog, W3C, Windows events and SNMP Traps generated by firewalls, servers, routers, switches, phone systems, PCs and more
> Increase network uptime and identify problems through real-time alerting
> Fast and cost-effective monitoring and management of the entire network
> SQL Server Auditing for SQL Server 2000, 2005, 2008 and also MSDE & SQL Express
> Unrivaled event scanning performance scalable to over 6 million events per hour
> Certified for Windows Server 2008; Supports Windows Vista
> Identify event patterns and preempt insider attacks through the powerful GFI EventsManager rules database
> Real-time alerts will avoid recovery costs that would otherwise result from network security attacks
> By taking a proactive approach, you will be reducing the risk to disrupt business continuity resulting from a security attack that could have been avoided through proper log management
> Increase productivity by reducing wasted manpower to go over all event logs manually
> Reduce administrative and technical overheads required to manage, archive and the cost to convert apparently meaningless event logs to significant security reports for management.
> Identify event patterns and preempt insider attacks through the powerful GFI EventsManager rules database
> Real-time alerts will avoid recovery costs that would otherwise result from network security attacks
> By taking a proactive approach, you will be reducing the risk to disrupt business continuity resulting

from a security attack that could have been avoided through proper log management

- Increase productivity by reducing wasted manpower to go over all event logs manually
- Reduce administrative and technical overheads required to manage, archive and the cost to convert apparently meaningless event logs to significant security reports for management.
- Monitor for critical security events network-wide - detect attacks & malicious network users
- Receive alerts about critical events on Exchange, ISA, SQL and IIS Servers
- Back up and clear event logs network-wide, and archive to a central database